H. Tanno et al.
11/25/03
Q78595
1 of 1

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００２年１１月２６日

出願番号
Application Number: 特願２００２－３４２７３５

[ST. 10/C]: [ＪＰ２００２－３４２７３５]

出願人
Applicant(s): 日本電気株式会社
エヌイーシーシステムテクノロジー株式会社

２００３年　８月２０日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００３－３０６８０２３

【書類名】　特許願
【整理番号】　64300936
【提出日】　平成14年11月26日
【あて先】　特許庁長官　太田　信一郎　殿
【国際特許分類】　G06F 17/30
G06F 17/60
【発明者】
【住所又は居所】　東京都港区芝五丁目７番１号　日本電気株式会社内
【氏名】　丹野　秀和
【発明者】
【住所又は居所】　東京都港区芝五丁目７番１号　日本電気株式会社内
【氏名】　関　義長
【発明者】
【住所又は居所】　大阪府大阪市中央区城見一丁目４番２４号　エヌイーシーシステムテクノロジー株式会社内
【氏名】　長谷井　伸次
【特許出願人】
【識別番号】　000004237
【氏名又は名称】　日本電気株式会社
【特許出願人】
【識別番号】　390001395
【氏名又は名称】　エヌイーシーシステムテクノロジー株式会社
【代理人】
【識別番号】　100086759
【弁理士】
【氏名又は名称】　渡辺　喜平
【手数料の表示】
【予納台帳番号】　013619
【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9001716

【包括委任状番号】　9005478

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　ネットワークを利用したソフトウェア資産管理漏れ検出方法、システム、サーバ、及びプログラム

【特許請求の範囲】

【請求項１】　コンピュータごとに、その基本情報及びインストールされているソフトウェア、修正パッチの適用状況を管理するソフトウェア資産管理から漏れているコンピュータを検出するためのネットワークを利用したソフトウェア資産管理漏れ検出方法であって、

所定のネットワークに接続された全てのコンピュータについて、各コンピュータを特定するための情報を保有するネットワーク接続コンピュータリストと、前記ソフトウェア資産管理の管理対象となっている全てのコンピュータについて、各コンピュータを特定するための情報を保有するソフトウェア資産管理リストとにもとづいて、前記ネットワーク接続コンピュータリストに存在し、かつ、前記ソフトウェア資産管理リストに存在しないコンピュータを抽出し、ソフトウェア資産管理漏れのコンピュータのリストを作成する

ことを特徴とするネットワークを利用したソフトウェア資産管理漏れ検出方法。

【請求項２】　請求項１記載のネットワークを利用したソフトウェア資産管理漏れ検出方法において、

前記ネットワーク接続コンピュータリスト及び前記ソフトウェア資産管理リストにもとづいて、前記ソフトウェア資産管理リストに存在し、かつ、前記ネットワーク接続コンピュータリストに存在しないコンピュータを抽出し、非使用状態となっているコンピュータのリストを作成する

ことを特徴とするネットワークを利用したソフトウェア資産管理漏れ検出方法。

【請求項３】　コンピュータごとに、その基本情報及びインストールされているソフトウェア、修正パッチの適用状況を管理するソフトウェア資産管理から漏れているコンピュータを検出するためのネットワークを利用したソフトウェア資産管理漏れ検出システムであって、

所定のネットワークに接続された全てのコンピュータについて、各コンピュータを特定するための情報を保有するネットワーク接続コンピュータリストを備えたネットワーク接続管理サーバと、

前記ソフトウェア資産管理の管理対象となっている全てのコンピュータについて、各コンピュータを特定するための情報を保有するソフトウェア資産管理リストを備えたソフトウェア資産管理サーバと、

前記ネットワーク接続コンピュータリスト及び前記ソフトウェア資産管理リストにもとづいて、前記ネットワーク接続コンピュータリストに存在し、かつ、前記ソフトウェア資産管理リストに存在しないコンピュータを抽出し、ソフトウェア資産管理漏れのコンピュータのリストを作成するソフトウェア資産管理漏れ検出サーバとを有する

ことを特徴とするネットワークを利用したソフトウェア資産管理漏れ検出システム。

【請求項４】　請求項３記載のネットワークを利用したソフトウェア資産管理漏れ検出システムにおいて、

前記ソフトウェア資産管理漏れ検出サーバが、

前記ネットワーク接続コンピュータリスト及び前記ソフトウェア資産管理リストにもとづいて、前記ソフトウェア資産管理リストに存在し、かつ、前記ネットワーク接続コンピュータリストに存在しないコンピュータを抽出し、非使用状態となっているコンピュータのリストを作成する

ことを特徴とするネットワークを利用したソフトウェア資産管理漏れ検出システム。

【請求項５】　コンピュータごとに、その基本情報及びインストールされているソフトウェア、修正パッチの適用状況を管理するソフトウェア資産管理から漏れているコンピュータを検出するためのネットワークを利用したソフトウェア資産管理漏れ検出サーバであって、

所定のネットワークに接続された全てのコンピュータについて、各コンピュータを特定するための情報を保有するネットワーク接続コンピュータリストを備えたネットワーク接続管理サーバから、前記ネットワーク接続コンピュータリスト

を受信するとともに、

前記ソフトウェア資産管理の管理対象となっている全てのコンピュータについて、各コンピュータを特定するための情報を保有するソフトウェア資産管理リストを備えたソフトウェア資産管理サーバから、前記ソフトウェア資産管理リストを受信し、

前記ネットワーク接続コンピュータリスト及び前記ソフトウェア資産管理リストにもとづいて、前記ネットワーク接続コンピュータリストに存在し、かつ、前記ソフトウェア資産管理リストに存在しないコンピュータを抽出し、ソフトウェア資産管理漏れのコンピュータのリストを作成する

ことを特徴とするネットワークを利用したソフトウェア資産管理漏れ検出サーバ。

【請求項６】　コンピュータごとに、その基本情報及びインストールされているソフトウェア、修正パッチの適用状況を管理するソフトウェア資産管理から漏れているコンピュータを検出するためのネットワークを利用したソフトウェア資産管理漏れ検出サーバであって、

所定のネットワークに接続された全てのコンピュータについて、各コンピュータを特定するための情報を保有するネットワーク接続コンピュータリストを作成するネットワーク接続管理部と、

前記ソフトウェア資産管理の管理対象となっている全てのコンピュータについて、各コンピュータを特定するための情報を保有するソフトウェア資産管理リストを作成するソフトウェア資産管理部と、

前記ネットワーク接続管理部から入力した前記ネットワーク接続コンピュータリスト及び前記ソフトウェア資産管理部から入力した前記ソフトウェア資産管理リストにもとづいて、前記ネットワーク接続コンピュータリストに存在し、かつ、前記ソフトウェア資産管理リストに存在しないコンピュータを抽出し、ソフトウェア資産管理漏れのコンピュータのリストを作成するソフトウェア資産管理漏れ検出部とを有する

ことを特徴とするネットワークを利用したソフトウェア資産管理漏れ検出サーバ。

【請求項７】　請求項５記載のネットワークを利用したソフトウェア資産管理漏れ検出サーバが、

前記ネットワーク接続コンピュータリスト及び前記ソフトウェア資産管理リストにもとづいて、前記ソフトウェア資産管理リストに存在し、かつ、前記ネットワーク接続コンピュータリストに存在しないコンピュータを抽出し、非使用状態となっているコンピュータのリストを作成する

ことを特徴とするネットワークを利用したソフトウェア資産管理漏れ検出サーバ。

【請求項８】　請求項６記載のネットワークを利用したソフトウェア資産管理漏れ検出サーバにおいて、

前記ソフトウェア資産管理漏れ検出部が、

前記ネットワーク接続コンピュータリスト及び前記ソフトウェア資産管理リストにもとづいて、前記ソフトウェア資産管理リストに存在し、かつ、前記ネットワーク接続コンピュータリストに存在しないコンピュータを抽出し、非使用状態となっているコンピュータのリストを作成する

ことを特徴とするネットワークを利用したソフトウェア資産管理漏れ検出サーバ。

【請求項９】　請求項５～８のいずれかに記載のネットワークを利用したソフトウェア資産管理漏れ検出サーバが、

前記ネットワーク接続コンピュータリスト及び前記ソフトウェア資産管理リストをソートし、このソートしたネットワーク接続コンピュータリスト及びソフトウェア資産管理リストにもとづいて、前記ソフトウェア資産管理漏れのコンピュータのリスト、又は、前記非使用状態となっているコンピュータのリストを作成する

ことを特徴とするネットワークを利用したソフトウェア資産管理漏れ検出サーバ。

【請求項１０】　コンピュータごとに、その基本情報及びインストールされているソフトウェア、修正パッチの適用状況を管理するソフトウェア資産管理から漏れているコンピュータを検出するためのネットワークを利用したソフトウェ

ア資産管理漏れ検出プログラムであって、

ソフトウェア資産管理漏れ検出サーバに、

所定のネットワークに接続された全てのコンピュータについて、各コンピュータを特定するための情報を保有するネットワーク接続コンピュータリストを備えたネットワーク接続管理サーバから、前記ネットワーク接続コンピュータリストを受信させるとともに、

前記ソフトウェア資産管理の管理対象となっている全てのコンピュータについて、各コンピュータを特定するための情報を保有するソフトウェア資産管理リストを備えたソフトウェア資産管理サーバから、前記ソフトウェア資産管理リストを受信させ、

前記ネットワーク接続コンピュータリスト及び前記ソフトウェア資産管理リストにもとづいて、前記ネットワーク接続コンピュータリストに存在し、かつ、前記ソフトウェア資産管理リストに存在しないコンピュータを抽出させ、ソフトウェア資産管理漏れのコンピュータのリストを作成させる

ことを特徴とするネットワークを利用したソフトウェア資産管理漏れ検出プログラム。

【請求項１１】　コンピュータごとに、その基本情報及びインストールされているソフトウェア、修正パッチの適用状況を管理するソフトウェア資産管理から漏れているコンピュータを検出するためのネットワークを利用したソフトウェア資産管理漏れ検出プログラムであって、

ソフトウェア資産管理漏れ検出サーバに、

所定のネットワークに接続された全てのコンピュータについて、各コンピュータを特定するための情報を保有するネットワーク接続コンピュータリストを作成させるとともに、

前記ソフトウェア資産管理の管理対象となっている全てのコンピュータについて、各コンピュータを特定するための情報を保有するソフトウェア資産管理リストを作成させ、

前記ネットワーク接続コンピュータリスト及び前記ソフトウェア資産管理リストにもとづいて、前記ネットワーク接続コンピュータリストに存在し、かつ、前

記ソフトウェア資産管理リストに存在しないコンピュータを抽出させ、ソフトウェア資産管理漏れのコンピュータのリストを作成させる

ことを特徴とするネットワークを利用したソフトウェア資産管理漏れ検出プログラム。

【請求項１２】　請求項１０又は１１記載のネットワークを利用したソフトウェア資産管理漏れ検出プログラムが、

ソフトウェア資産管理漏れ検出サーバに、

前記ネットワーク接続コンピュータリスト及び前記ソフトウェア資産管理リストにもとづいて、前記ソフトウェア資産管理リストに存在し、かつ、前記ネットワーク接続コンピュータリストに存在しないコンピュータを抽出させ、非使用状態となっているコンピュータのリストを作成させる

ことを特徴とするネットワークを利用したソフトウェア資産管理漏れ検出プログラム。

【請求項１３】　請求項１０～１２のいずれかに記載のネットワークを利用したソフトウェア資産管理漏れ検出プログラムが、

ソフトウェア資産管理漏れ検出サーバに、

前記ネットワーク接続コンピュータリスト及び前記ソフトウェア資産管理リストをソートさせ、このソートされたネットワーク接続コンピュータリスト及びソフトウェア資産管理リストにもとづいて、前記ソフトウェア資産管理漏れのコンピュータのリスト、又は、前記非使用状態となっているコンピュータのリストを作成させる

ことを特徴とするネットワークを利用したソフトウェア資産管理漏れ検出プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、コンピュータごとに、その基本情報及びインストールされているソフトウェア、修正パッチの適用状況を管理するソフトウェア資産管理から、管理すべきコンピュータが漏れることを防止するネットワークを利用したソフトウェ

ア資産管理漏れ検出方法、システム、サーバ及びプログラムに関する。

【０００２】

【従来の技術】

近年、コンピュータは、企業や団体などにおいて、その業務上広く使用されている。このコンピュータの使用にあたっては、その使用の目的にあったソフトウェアを用いる必要があるため、これらの企業等は、コンピュータに様々なソフトウェアをインストールして使用している。

そのため、企業等においては、購入したソフトウェアライセンスを適切に管理し、組織内で不正にソフトウェアをコピーして利用されることのないような施策を講じる必要がある。

しかし、ソフトウェアはほとんどの場合、ひとつの媒体から複数のコンピュータに簡単にインストールすることが可能であるため、ライセンス数を超えてインストールされていないかどうかを正確に把握する作業は膨大なものになり、また調査した結果を維持管理することも組織が大きくなるにつれて非常に困難なものになるという問題があった。

【０００３】

また、最近ではコンピュータの多くがネットワークに接続され、ネットワークを介して情報のやり取りが行われている。

このような状況においては、電子メールやＷｅｂアクセスなどを媒介とするウィルスの感染を防ぐために、ネットワークに接続されているコンピュータにインストールされているＯＳやアプリケーションソフトウェアが、ソフトウェアの開発元が提供している修正パッチを適用することなどによってセキュリティ上問題がない状態になっているかを管理する必要がある。

しかし、ソフトウェアライセンス管理の問題と同様に、ＯＳやアプリケーションが適切に更新されているかどうかを把握するには非常に多大な作業が必要となるという問題があった。

【０００４】

これらの問題に対し、ネットワークに接続されている各コンピュータ上で、コンピュータの基本情報（ホスト名，ネットワークアドレス等）やインストールさ

れているソフトウェアのリスト情報等を収集するソフトウェア資産管理用のクライアントソフトウェアを動作させ、収集した情報をソフトウェア資産管理用のサーバに送信することにより、ソフトウェア資産情報が自動的に一元管理されるようにすることを可能とする方法等が提案されている（例えば、特許文献１～３参照。）。また、ソフトウェアの修正パッチを専用のサーバで管理し、コンピュータがパッチ未使用の場合に自動的に修正パッチをダウンロードして適用する方法等が提案されている（例えば、特許文献４，５参照。）

【０００５】

【特許文献１】

特開２００１－２２２４２４号公報

【特許文献２】

特開２００１－２９０９３７号公報

【特許文献３】

特開２００２－２７９１６５号公報

【特許文献４】

特開２０００－２５０７４３号公報

【特許文献５】

特開２００２－５５８３９号公報

【０００６】

【発明が解決しようとする課題】

しかしながら、このような従来の方法では、各コンピュータ上でソフトウェア資産管理用のクライアントソフトウェアや、修正パッチをダウンロードして適用するクライアントソフトウェアがインストールされ動作していること、又はＯＳやアプリケーションソフトウェアがこのようなクライアントソフトウェアと同等の機能を有していることが前提となっており、クライアントソフトウェアが動作していないコンピュータはソフトウェア資産管理情報から漏れてしまい、ソフトウェアの不正利用を見過ごしたり、セキュリティ上問題のある状態のコンピュータを見過ごしたりする恐れがあるという問題があった。

【０００７】

本発明は、上記の事情にかんがみなされたものであり、コンピュータごとに、その基本情報及びインストールされているソフトウェア、修正パッチの適用状況を管理するソフトウェア資産管理から、管理すべきコンピュータが漏れることを防止することによって、ＯＳやアプリケーションのパッチ適用状態が不明でセキュリティ上問題のある可能性の高いコンピュータを検出することを可能とするネットワークを利用したソフトウェア資産管理漏れ検出方法、システム、サーバ及びプログラムの提供を目的とする。

【０００８】

【課題を解決するための手段】

上記目的を達成するため、本発明の請求項１記載のネットワークを利用したソフトウェア資産管理漏れ検出方法は、コンピュータごとに、その基本情報及びインストールされているソフトウェア、修正パッチの適用状況を管理するソフトウェア資産管理から漏れているコンピュータを検出するためのネットワークを利用したソフトウェア資産管理漏れ検出方法であって、所定のネットワークに接続された全てのコンピュータについて、各コンピュータを特定するための情報を保有するネットワーク接続コンピュータリストと、ソフトウェア資産管理の管理対象となっている全てのコンピュータについて、各コンピュータを特定するための情報を保有するソフトウェア資産管理リストとにもとづいて、ネットワーク接続コンピュータリストに存在し、かつ、ソフトウェア資産管理リストに存在しないコンピュータを抽出し、ソフトウェア資産管理漏れのコンピュータのリストを作成する方法としてある。

【０００９】

ネットワークを利用したソフトウェア資産管理漏れ検出方法をこのような方法にすれば、ソフトウェア資産管理情報とは別にネットワークに接続されているコンピュータを漏れなく含むリストを作成し、ネットワークアドレスなどネットワーク上でコンピュータを一意に識別することが可能な情報を用いることで、ソフトウェア資産管理から漏れているコンピュータを見つけ出すことができる。

このため、ソフトウェア資産管理から漏れているコンピュータを容易に洗い出すことが可能となる。

【００１０】

また、ネットワークに接続されているコンピュータを漏れなく含むリストを作成する手段を、従来のソフトウェア資産管理システムから独立して構成し、ソフトウェア資産管理漏れのコンピュータを検出することができる。

そして、このソフトウェア資産管理漏れのコンピュータに対して、従来のソフトウェア資産管理システムを適用することが可能となる。

このため、従来のソフトウェア資産管理システムを大幅に変更することなくソフトウェア資産管理情報の漏れを防止することが可能となる。

【００１１】

その結果、ＯＳやソフトウェアのバージョンやパッチ適用状態等も同時に管理するソフトウェア資産管理において、ネットワークに接続されたコンピュータを漏れなく含んだリストを用いることによって、管理漏れを防ぐことが可能となる。

このため、ＯＳやソフトウェアのバージョンやパッチ適用状態等が不明なコンピュータを検出し、パッチ適用状態が最新ではなくセキュリティホールとなりうるコンピュータがネットワークに接続されたままになることを防止することが可能となる。

【００１２】

また、ネットワーク接続コンピュータリストとソフトウェア資産管理リストを１日ごとなど適切な間隔で定期的に更新して比較することにより、新規にネットワークに接続されたコンピュータがソフトウェア資産管理下にあるかどうかを確認することができる。

このため、ソフトウェア資産管理外のコンピュータや不正なコンピュータが接続された場合、管理外コンピュータとして早期に発見することが可能となる。

【００１３】

なお、基本情報とは、ネットワークアドレスやコンピュータ名等の情報を意味している。また、この基本情報としては、各コンピュータを特定するための一の情報のみであってもかまわない。

また、所定のネットワークとは、例えば、社内ＬＡＮやＶＰＮなどであり、企

業や官公庁、学校、その他の団体や個人等によって、その管理の対象とされるネットワークを意味している。

【００１４】

本発明の請求項２記載のネットワークを利用したソフトウェア資産管理漏れ検出方法は、請求項１記載のネットワークを利用したソフトウェア資産管理漏れ検出方法において、ネットワーク接続コンピュータリスト及びソフトウェア資産管理リストにもとづいて、ソフトウェア資産管理リストに存在し、かつ、ネットワーク接続コンピュータリストに存在しないコンピュータを抽出し、非使用状態となっているコンピュータのリストを作成する方法としてある。

【００１５】

ネットワークを利用したソフトウェア資産管理漏れ検出方法をこのような方法にすれば、非使用コンピュータリストを作成することができるため、以前使用されていたが、現在は使用されていないコンピュータを洗い出すことが可能となる。

また、ソフトウェア資産管理漏れ検出リストと非使用コンピュータリストの双方を作成することによって、ソフトウェア資産管理から漏れているコンピュータを検出することができるとともに、現在未使用のソフトウェアの一覧を取得することも可能となり、ソフトウェア資産管理をより厳密に行うことが容易となる。

【００１６】

本発明の請求項３記載のネットワークを利用したソフトウェア資産管理漏れ検出システムは、コンピュータごとに、その基本情報及びインストールされているソフトウェア、修正パッチの適用状況を管理するソフトウェア資産管理から漏れているコンピュータを検出するためのネットワークを利用したソフトウェア資産管理漏れ検出システムであって、所定のネットワークに接続された全てのコンピュータについて、各コンピュータを特定するための情報を保有するネットワーク接続コンピュータリストを備えたネットワーク接続管理サーバと、ソフトウェア資産管理の管理対象となっている全てのコンピュータについて、各コンピュータを特定するための情報を保有するソフトウェア資産管理リストを備えたソフトウェア資産管理サーバと、ネットワーク接続コンピュータリスト及びソフトウェア

資産管理リストにもとづいて、ネットワーク接続コンピュータリストに存在し、かつ、ソフトウェア資産管理リストに存在しないコンピュータを抽出し、ソフトウェア資産管理漏れのコンピュータのリストを作成するソフトウェア資産管理漏れ検出サーバとを有する構成としてある。

【００１７】

ネットワークを利用したソフトウェア資産管理漏れ検出システムをこのような構成にすれば、ソフトウェア資産管理サーバにより管理されるソフトウェア資産管理リストと、ネットワーク接続管理サーバによって作成されたネットワーク接続コンピュータリストにもとづいて、ネットワークアドレスなどネットワーク上でコンピュータを一意に識別することが可能な情報を用いることで、ネットワークに接続されているにもかかわらず、ソフトウェア資産管理が行われていないコンピュータを容易に見つけ出すことが可能となる。

その結果、ＯＳやソフトウェアのバージョンやパッチ適用状態等が不明なコンピュータを検出し、パッチ適用状態が最新ではなくセキュリティホールとなりうるコンピュータがネットワークに接続されたままになることを防止することが可能となる。

【００１８】

また、ネットワークを利用したソフトウェア資産管理漏れ検出システムをこのような構成にすることによって、従来のソフトウェア資産管理システムに対して、大きな変更を行うことなく、その管理対象の漏れを防止することが可能となる。

さらに、ソフトウェア資産管理外のコンピュータや不正なコンピュータが接続された場合に、管理外のコンピュータとして早期に発見することも可能となる。

【００１９】

本発明の請求項４記載のネットワークを利用したソフトウェア資産管理漏れ検出システムは、請求項３記載のネットワークを利用したソフトウェア資産管理漏れ検出システムにおいて、ソフトウェア資産管理漏れ検出サーバが、ネットワーク接続コンピュータリスト及びソフトウェア資産管理リストにもとづいて、ソフトウェア資産管理リストに存在し、かつ、ネットワーク接続コンピュータリスト

に存在しないコンピュータを抽出し、非使用状態となっているコンピュータのリストを作成する構成としてある。

【００２０】

ネットワークを利用したソフトウェア資産管理漏れ検出システムをこのような構成にすれば、以前使用されていたが、現在は使用されていないコンピュータを洗い出すことが可能となる。

このため、ソフトウェア資産管理から漏れているコンピュータを検出することに加え、現在未使用のソフトウェアの一覧を取得することも可能となる。

【００２１】

本発明の請求項５記載のネットワークを利用したソフトウェア資産管理漏れ検出サーバは、コンピュータごとに、その基本情報及びインストールされているソフトウェア、修正パッチの適用状況を管理するソフトウェア資産管理から漏れているコンピュータを検出するためのネットワークを利用したソフトウェア資産管理漏れ検出サーバであって、所定のネットワークに接続された全てのコンピュータについて、各コンピュータを特定するための情報を保有するネットワーク接続コンピュータリストを備えたネットワーク接続管理サーバから、ネットワーク接続コンピュータリストを受信するとともに、ソフトウェア資産管理の管理対象となっている全てのコンピュータについて、各コンピュータを特定するための情報を保有するソフトウェア資産管理リストを備えたソフトウェア資産管理サーバから、ソフトウェア資産管理リストを受信し、ネットワーク接続コンピュータリスト及びソフトウェア資産管理リストにもとづいて、ネットワーク接続コンピュータリストに存在し、かつ、ソフトウェア資産管理リストに存在しないコンピュータを抽出し、ソフトウェア資産管理漏れのコンピュータのリストを作成する構成としてある。

【００２２】

ネットワークを利用したソフトウェア資産管理漏れ検出サーバをこのような構成にすれば、ネットワーク接続管理サーバからのネットワーク接続コンピュータリストと、ソフトウェア資産管理サーバからのソフトウェア資産管理リストにもとづいて、容易にソフトウェア資産管理漏れのコンピュータを検出することが可

能となる。

また、従来のソフトウェア資産管理システムが、ソフトウェア資産管理サーバに保有されている場合であっても、このソフトウェア資産管理サーバに対する変更をほとんど加える必要がない。

さらに、セキュリティホールとなりうるコンピュータがネットワークに接続されたままになることを防止し、ソフトウェア資産管理外のコンピュータや不正なコンピュータが接続された場合は、これを早期に発見することが可能となる。

【００２３】

本発明の請求項６記載のネットワークを利用したソフトウェア資産管理漏れ検出サーバは、コンピュータごとに、その基本情報及びインストールされているソフトウェア、修正パッチの適用状況を管理するソフトウェア資産管理から漏れているコンピュータを検出するためのネットワークを利用したソフトウェア資産管理漏れ検出サーバであって、所定のネットワークに接続された全てのコンピュータについて、各コンピュータを特定するための情報を保有するネットワーク接続コンピュータリストを作成するネットワーク接続管理部と、ソフトウェア資産管理の管理対象となっている全てのコンピュータについて、各コンピュータを特定するための情報を保有するソフトウェア資産管理リストを作成するソフトウェア資産管理部と、ネットワーク接続管理部から入力したネットワーク接続コンピュータリスト及びソフトウェア資産管理部から入力したソフトウェア資産管理リストにもとづいて、ネットワーク接続コンピュータリストに存在し、かつ、ソフトウェア資産管理リストに存在しないコンピュータを抽出し、ソフトウェア資産管理漏れのコンピュータのリストを作成するソフトウェア資産管理漏れ検出部とを有する構成としてある。

【００２４】

ネットワークを利用したソフトウェア資産管理漏れ検出サーバをこのような構成にすれば、一台のサーバにおいて、ソフトウェア資産管理漏れ検出リストを作成することが可能となる。

すなわち、従来のソフトウェア資産管理システムを構成するサーバに対し、従来のソフトウェア資産管理システムの付加的機能として、上記構成を加えること

により、本発明におけるソフトウェア資産管理漏れ検出リストの作成を行わせるようにすることができる。

【００２５】

本発明の請求項７記載のネットワークを利用したソフトウェア資産管理漏れ検出サーバは、請求項５記載のネットワークを利用したソフトウェア資産管理漏れ検出サーバが、ネットワーク接続コンピュータリスト及びソフトウェア資産管理リストにもとづいて、ソフトウェア資産管理リストに存在し、かつ、ネットワーク接続コンピュータリストに存在しないコンピュータを抽出し、非使用状態となっているコンピュータのリストを作成する構成としてある。

【００２６】

また、本発明の請求項８記載のネットワークを利用したソフトウェア資産管理漏れ検出サーバは、請求項６記載のネットワークを利用したソフトウェア資産管理漏れ検出サーバにおいて、ソフトウェア資産管理漏れ検出部が、ネットワーク接続コンピュータリスト及びソフトウェア資産管理リストにもとづいて、ソフトウェア資産管理リストに存在し、かつ、ネットワーク接続コンピュータリストに存在しないコンピュータを抽出し、非使用状態となっているコンピュータのリストを作成する構成としてある。

【００２７】

ネットワークを利用したソフトウェア資産管理漏れ検出サーバをこれらのような構成にすれば、以前使用されていたが、現在は使用されていないコンピュータを洗い出すことができる。

すなわち、ソフトウェア資産管理から漏れているコンピュータを検出することに加えて、現在未使用のソフトウェアの一覧を取得することも可能となる。

【００２８】

本発明の請求項９記載のネットワークを利用したソフトウェア資産管理漏れ検出サーバは、請求項５～８のいずれかに記載のネットワークを利用したソフトウェア資産管理漏れ検出サーバが、ネットワーク接続コンピュータリスト及びソフトウェア資産管理リストをソートし、このソートしたネットワーク接続コンピュータリスト及びソフトウェア資産管理リストにもとづいて、ソフトウェア資産管

理漏れのコンピュータのリスト、又は、非使用状態となっているコンピュータのリストを作成する構成としてある。

【００２９】

ネットワークを利用したソフトウェア資産管理漏れ検出サーバをこのような構成にすれば、例えば、ネットワーク接続コンピュータリスト及びソフトウェア資産管理リストのそれぞれを、ネットワークアドレスなどにもとづいて昇順、又は降順にソートすることによって、ソフトウェア資産管理漏れ検出リストの作成において、逐次探索アルゴリズムを利用する代わりに、二分探索アルゴリズムなどを利用した処理を行うことが可能となる。

このため、ソフトウェア資産管理漏れ検出リストや非使用コンピュータリストを生成する処理をより高速化することが可能となる。

【００３０】

本発明の請求項１０記載のネットワークを利用したソフトウェア資産管理漏れ検出プログラムは、コンピュータごとに、その基本情報及びインストールされているソフトウェア、修正パッチの適用状況を管理するソフトウェア資産管理から漏れているコンピュータを検出するためのネットワークを利用したソフトウェア資産管理漏れ検出プログラムであって、ソフトウェア資産管理漏れ検出サーバに、所定のネットワークに接続された全てのコンピュータについて、各コンピュータを特定するための情報を保有するネットワーク接続コンピュータリストを備えたネットワーク接続管理サーバから、ネットワーク接続コンピュータリストを受信させるとともに、ソフトウェア資産管理の管理対象となっている全てのコンピュータについて、各コンピュータを特定するための情報を保有するソフトウェア資産管理リストを備えたソフトウェア資産管理サーバから、ソフトウェア資産管理リストを受信させ、ネットワーク接続コンピュータリスト及びソフトウェア資産管理リストにもとづいて、ネットワーク接続コンピュータリストに存在し、かつ、ソフトウェア資産管理リストに存在しないコンピュータを抽出させ、ソフトウェア資産管理漏れのコンピュータのリストを作成させる構成としてある。

【００３１】

ネットワークを利用したソフトウェア資産管理漏れ検出プログラムをこのよう

な構成にすれば、ソフトウェア資産管理漏れ検出サーバに、ネットワーク接続管理サーバからのネットワーク接続コンピュータリストと、ソフトウェア資産管理サーバからのソフトウェア資産管理リストにもとづいて、容易にソフトウェア資産管理漏れのコンピュータを検出させることが可能となる。

このため、ＯＳやソフトウェアのバージョンやパッチ適用状態等も同時に管理するソフトウェア資産管理において、本発明のネットワークに接続されたコンピュータを漏れなく含んだリストを作成することにより、その管理漏れを防ぐことが可能となる。

【００３２】

本発明の請求項１１記載のネットワークを利用したソフトウェア資産管理漏れ検出プログラムは、コンピュータごとに、その基本情報及びインストールされているソフトウェア、修正パッチの適用状況を管理するソフトウェア資産管理から漏れているコンピュータを検出するためのネットワークを利用したソフトウェア資産管理漏れ検出プログラムであって、ソフトウェア資産管理漏れ検出サーバに、所定のネットワークに接続された全てのコンピュータについて、各コンピュータを特定するための情報を保有するネットワーク接続コンピュータリストを作成させるとともに、ソフトウェア資産管理の管理対象となっている全てのコンピュータについて、各コンピュータを特定するための情報を保有するソフトウェア資産管理リストを作成させ、ネットワーク接続コンピュータリスト及びソフトウェア資産管理リストにもとづいて、ネットワーク接続コンピュータリストに存在し、かつ、ソフトウェア資産管理リストに存在しないコンピュータを抽出させ、ソフトウェア資産管理漏れのコンピュータのリストを作成させる構成としてある。

【００３３】

ネットワークを利用したソフトウェア資産管理漏れ検出プログラムをこのような構成にすれば、一台のソフトウェア資産管理漏れ検出サーバに、ソフトウェア資産管理漏れ検出リストを作成させることが可能となる。

そして、これによって、ＯＳやソフトウェアのバージョンやパッチ適用状態等も同時に管理するソフトウェア資産管理において、その管理漏れを防ぐことが可能となる。

【００３４】

本発明の請求項１２記載のネットワークを利用したソフトウェア資産管理漏れ検出プログラムは、請求項１０又は１１記載のネットワークを利用したソフトウェア資産管理漏れ検出プログラムが、ソフトウェア資産管理漏れ検出サーバに、ネットワーク接続コンピュータリスト及びソフトウェア資産管理リストにもとづいて、ソフトウェア資産管理リストに存在し、かつ、ネットワーク接続コンピュータリストに存在しないコンピュータを抽出させ、非使用状態となっているコンピュータのリストを作成させる構成としてある。

【００３５】

ネットワークを利用したソフトウェア資産管理漏れ検出プログラムをこのような構成にすれば、ソフトウェア資産管理漏れ検出サーバに、以前使用されていたが、現在は使用されていないコンピュータを洗い出させることができる。

また、これによって、ソフトウェア資産管理漏れ検出サーバに、現在未使用のソフトウェアの一覧を出力させることが可能となる。

【００３６】

本発明の請求項１３記載のネットワークを利用したソフトウェア資産管理漏れ検出プログラムは、請求項１０～１２のいずれかに記載のネットワークを利用したソフトウェア資産管理漏れ検出プログラムが、ソフトウェア資産管理漏れ検出サーバに、ネットワーク接続コンピュータリスト及びソフトウェア資産管理リストをソートさせ、このソートされたネットワーク接続コンピュータリスト及びソフトウェア資産管理リストにもとづいて、ソフトウェア資産管理漏れのコンピュータのリスト、又は、非使用状態となっているコンピュータのリストを作成させる構成としてある。

【００３７】

ネットワークを利用したソフトウェア資産管理漏れ検出プログラムをこのような構成にすれば、ソフトウェア資産管理漏れ検出サーバに、ネットワーク接続コンピュータリスト及びソフトウェア資産管理リストをソートさせた後に、ソフトウェア資産管理漏れ検出リスト又は非使用コンピュータリストを作成させることが可能となる。

これによって、その作成処理を高速化させることが可能となる。

【００３８】

【発明の実施の形態】

以下、本発明の実施形態につき、図面を参照して説明する。

［第一実施形態］

まず、本発明の第一実施形態について、図１及び図２を参照して説明する。図１は、本発明の第一実施形態のネットワークを利用したソフトウェア資産管理漏れ検出システムの構成を示すブロック図である。また、図２は、同システムにおけるネットワーク接続コンピュータリスト及びソフトウェア資産管理リストを示す図である。

図１に示すように、ネットワークを利用したソフトウェア資産管理漏れ検出システムは、ネットワーク接続管理サーバ１０、ソフトウェア資産管理サーバ２０、及びソフトウェア資産管理漏れ検出サーバ３０により構成されている。

本実施形態においては、これらのサーバが、物理ネットワークとしてＥｔｈｅｒｎｅｔ（登録商標）、ネットワークプロトコルとしてＴＣＰ／ＩＰ（Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｃｏｎｔｒｏｌ　Ｐｒｏｔｏｃｏｌ／Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）を用いて接続されているものとしているが、これに限定されるものではない。

【００３９】

ネットワーク接続管理サーバ１０は、ネットワークに接続されているコンピュータを管理するサーバで、ネットワーク接続コンピュータリスト１００を保有している。

このネットワーク接続コンピュータリスト１００は、ネットワークに接続されているコンピュータを漏れなく含むようにリストアップできる手段であれば、どのような手段を用いて作成してもかまわない。

【００４０】

例えば、物理ネットワークにＥｔｈｅｒｎｅｔ（登録商標）、ネットワークプロトコルにＴＣＰ／ＩＰを用いる場合には、コンピュータがネットワークに接続して通信を行う際に、ＡＲＰ（Ａｄｄｒｅｓｓ　Ｒｅｓｏｌｕｔｉｏｎ　Ｐｒｏ

ｔｏｃｏｌ）をブロードキャストして接続先コンピュータのＭＡＣ（Ｍｅｄｉａ Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ）アドレスを特定する仕組みを利用することができる。

すなわち、各ブロードキャストドメインにパケットを監視する装置を設置してＡＲＰパケットを監視し、ＡＲＰパケットに含まれるＭＡＣアドレスとＩＰアドレスでコンピュータを検知してリストアップする。

そして、検知したＩＰアドレスを用いてＤＮＳ（Ｄｏｍａｉｎ　Ｎａｍｅ　Ｓｙｓｔｅｍ）へ問い合わせ、コンピュータ名を特定することで、ネットワークに接続されたコンピュータを漏れなく含むネットワーク接続コンピュータリスト１００を生成するという手段を用いることができる。

【００４１】

ソフトウェア資産管理サーバ２０は、組織内で購入利用されているソフトウェア資産の利用状況を管理するサーバであり、ソフトウェア資産管理リスト２００を保有している。

このソフトウェア資産管理リスト２００は、各コンピュータにインストールされているＯＳ（Ｏｐｅｒａｔｉｎｇ　Ｓｙｓｔｅｍ）やアプリケーションの種類や名前、パッチ適用状態などのソフトウェア資産管理情報と、ＭＡＣアドレスやＩＰアドレス、コンピュータ名などのコンピュータの基本情報をリストアップできる手段であれば、どのような手段を用いて作成してもかまわない。

【００４２】

例えば、各コンピュータにおいて、ソフトウェア資産管理情報とコンピュータの基本情報を調査するエージェントソフトを動作させ、調査結果をソフトウェア資産管理サーバ２００に送信させる。

そして、この各コンピュータから送信されてきた情報にもとづいて、ソフトウェア資産管理サーバ２０に、ソフトウェア資産管理リスト２００を生成させるという手段を用いることができる。

【００４３】

ソフトウェア資産管理漏れ検出サーバ３０は、ネットワーク接続管理サーバ１０からネットワーク接続コンピュータリスト１００を受信するとともに、ソフト

ウェア資産管理サーバ２０からソフトウェア資産管理リスト２００を受信する。

そして、Ｅｔｈｅｒｎｅｔ（登録商標）での通信でコンピュータを識別するために利用するＭＡＣアドレスをキーとして、ネットワーク接続コンピュータリスト１００とソフトウェア資産管理リスト２００とを比較し、ソフトウェア資産管理リスト２００から漏れているコンピュータの洗い出しを行う。

【００４４】

このコンピュータの洗い出しについて、図２を用いて説明する。同図において、ネットワーク接続コンピュータリスト１００は、ネットワークに接続されたコンピュータを漏れなく検出する手段を用いて生成されたものであり、ネットワークアドレス１１１～１１ｍ、及びこれに対応するコンピュータ名１２１～１２ｍを有している。

また、ソフトウェア資産管理情報リスト２００は、各コンピュータ単位でコンピュータの基本情報やインストールされているＯＳ、アプリケーションソフト等を整理分類したものである。ここでは、基本情報として、ネットワークアドレスとコンピュータ名が登録されている。

【００４５】

コンピュータの洗い出しにあたっては、ネットワーク接続コンピュータリスト１００におけるネットワークアドレス１１１～１１ｍと、ソフトウェア資産管理情報リスト２００におけるネットワークアドレス２１１～２１ｎを比較し、１１１～１１ｍに含まれており２１１～２１ｎに含まれていないアドレスを持つコンピュータはソフトウェア資産管理情報から漏れているコンピュータと判断する。

この方法により、ネットワークに接続されているコンピュータで利用されているソフトウェア資産の管理漏れを防止することが容易となり、またＯＳやアプリケーションのパッチ適用状態が不明なコンピュータがネットワークに接続されたままとなりセキュリティ上問題となる状況を防止することが容易となる。

【００４６】

次に、本実施形態のネットワークを利用したソフトウェア資産管理漏れ検出サーバ３０における処理手順につき、図３を参照して説明する。同図は、本実施形態のネットワークを利用したソフトウェア資産管理漏れ検出システムにおける処

理手順を示すフローチャートである。

まず、同フローチャートにおける処理に先立ち、ソフトウェア資産管理漏れ検出サーバ３０は、ネットワーク接続管理サーバ１０からネットワーク接続コンピュータリスト１００を、ソフトウェア資産管理サーバ２０からソフトウェア資産管理リスト２００を受信する。

そして、ソフトウェア資産管理漏れ検出サーバ３０は、これらのリストにもとづいて、以下に示すように、ソフトウェア資産管理情報から漏れているコンピュータの洗い出しを行う。なお、図３のフローチャートにおける動作の主体は、ソフトウェア資産管理漏れ検出サーバ３０であるが、以下の説明においては、その記載を省略する。

【００４７】

まず、ネットワーク接続コンピュータリスト１００の先頭に記述されているコンピュータのＭＡＣアドレス情報を取り出す（ステップＡ１）。引き続くステップＡ２～Ａ６までの動作は、この取り出したＭＡＣアドレス１１ｉを持つコンピュータが、ソフトウェア資産管理リスト２００に含まれているかどうかを判断し、含まれていない場合はソフトウェア資産管理漏れコンピュータリスト３００に追加するという動作を表している。

【００４８】

すなわち、ソフトウェア資産管理リスト２００の先頭に記述されているコンピュータのＭＡＣアドレス情報を取り出す（ステップＡ２）。

そして、ステップＡ１で取り出したＭＡＣアドレスとステップＡ２で取り出したＭＡＣアドレスの比較を行い（ステップＡ３）、両者が同じであれば、接続コンピュータリスト１００から取り出したＭＡＣアドレス１１ｉに該当するコンピュータが、ソフトウェア資産管理リスト２００に含まれていると判断し、ステップＡ７へ進む。

【００４９】

また、ＭＡＣアドレスが異なる場合は、ステップＡ３における比較で用いたＭＡＣアドレスのうち、ソフトウェア資産管理リスト２００から取り出したＭＡＣアドレス２１ｊが、ソフトウェア資産管理リスト２００の最後のコンピュータの

ＭＡＣアドレスであるかどうかを判断する（ステップＡ４）。

そして、ＭＡＣアドレス２１ｊが、リストの最後のコンピュータのＭＡＣアドレスでなければ、リスト２００の次のコンピュータのＭＡＣアドレスを取り出して（ステップＡ５）、再びステップＡ３からの処理を実行する。

【００５０】

ＭＡＣアドレス２１ｊが、資産管理リスト２００の最後のコンピュータのＭＡＣアドレスであれば、ネットワーク接続コンピュータリスト１００から取り出したＭＡＣアドレス１１ｉに該当するコンピュータが、ソフトウェア資産管理リスト２００に含まれていないと判断し、ステップＡ６に進む。

そして、ＭＡＣアドレス１１ｉのコンピュータの情報をネットワーク接続コンピュータリスト１００から取り出し、ソフトウェア資産管理漏れコンピュータリスト３００へ追加して（ステップＡ６）、ステップＡ７に進む。

【００５１】

そして、ＭＡＣアドレス１１ｉが、ネットワーク接続コンピュータリスト１００の最後のコンピュータのＭＡＣアドレスであるかどうかを判断し（ステップＡ７）、ＭＡＣアドレス１１ｉが、リスト１００の最後のコンピュータのＭＡＣアドレスでなければ、次のコンピュータリストのＭＡＣアドレスを取り出して（ステップＡ８）、ステップＡ２～Ａ６の処理を繰り返す。

ＭＡＣアドレス１１ｉが、リスト１００の最後のコンピュータのＭＡＣアドレスの場合は、このネットワーク接続コンピュータリスト１００に含まれるすべてのコンピュータに対して、ソフトウェア資産管理リスト２００に含まれているかどうかを判断したことになるため、処理を終了する。

【００５２】

次に、図４及び図５を用いて、本実施形態のネットワークを利用したソフトウェア資源管理漏れ検出システムの処理手順について、具体例を用いて説明する。

図４は、本実施形態のネットワークを利用したソフトウェア資源管理漏れ検出システムにおけるネットワーク接続コンピュータリスト及びソフトウェア資産管理リストの具体例を示す図である。図５は、同システムにおけるソフトウェア資産管理漏れのコンピュータのリスト、すなわちソフトウェア資産管理漏れ検出リ

ストの具体例を示す図である。

以下に、図４に示すネットワーク接続コンピュータリスト１００、及びソフトウェア資産管理リスト２００を用いて、図３に示す上述の処理手順を実行した場合につき、具体的に説明する。

【００５３】

まず、ステップＡ１において、ネットワーク接続コンピュータリスト１００からリストの先頭のＭＡＣアドレス「００：００：４ｃ：１１：１１：１１」を取り出す。

そしてステップＡ２において、ソフトウェア資産管理リスト２００からリストの先頭のＭＡＣアドレス「００：００：４ｃ：５５：５５：５５」を取り出す。

【００５４】

次に、ステップＡ３で、取り出したＭＡＣアドレスの比較を行う。この場合、それぞれのリストから取り出したＭＡＣアドレスが異なっているため、ステップＡ４に進む。

ステップＡ４では、ソフトウェア資産管理リスト２００から取り出したＭＡＣアドレスがリストの最後のものかを判断する。この場合は、リストの最後ではないので、ステップＡ５に進み、リストの次のＭＡＣアドレス「００：００：４ｃ：１１：１１：１１」を取り出してステップＡ３に戻る。

【００５５】

次のステップＡ３でのＭＡＣアドレスの比較では、ＭＡＣアドレスが一致しているため、ステップＡ７に進む。

ステップＡ７では、ネットワーク接続コンピュータリストから取り出したＭＡＣアドレスが、リスト１００の最後のものかを判断する。この場合はリスト１００の最後のものではないため、ステップＡ８に進み、リスト１００の次のＭＡＣアドレス「００：００：４ｃ：２２：２２：２２」を取り出してステップＡ２に戻る。

【００５６】

これ以降の動作は、ネットワーク接続コンピュータリスト１００から取り出しＭＡＣアドレスが「００：００：４ｃ：１１：１１：１１」の場合と同様である

。

しかし、ＭＡＣアドレス「００：００：４ｃ：２２：２２：２２」のコンピュータは、ソフトウェア資産管理リスト２００に登録されていない。

このため、ソフトウェア資産管理リスト２００の最後のコンピュータである「００：００：４ｃ：７７：７７：７７」のＭＡＣアドレスが処理される場合は、ステップＡ４から、ステップＡ６に処理が進む。そして、ソフトウェア資産管理漏れリスト３００に、ＭＡＣアドレスが「００：００：４ｃ：２２：２２：２２」のコンピュータの情報が追加される。

【００５７】

同様に、ネットワーク接続コンピュータリストに登録されているコンピュータのうち、ＭＡＣアドレスが「００：００：４ｃ：５５：５５：５５」、「００：００：４ｃ：７７：７７：７７」のコンピュータに関しては、ソフトウェア資産管理リスト２００にも登録されている。

このため、これらのコンピュータについては、ＭＡＣアドレスが、「００：００：４ｃ：１１：１１：１１」のコンピュータの時と同様の動作となる。

【００５８】

また、ＭＡＣアドレスが「００：００：４ｃ：ｂｂ：ｂｂ：ｂｂ」のコンピュータに関しては、ソフトウェア資産管理リスト２００に登録されていないため、ＭＡＣアドレスが「００：００：４ｃ：２２：２２：２２」のコンピュータの時と同様の動作となる。

ただし、このＭＡＣアドレスが「００：００：４ｃ：ｂｂ：ｂｂ：ｂｂ」のコンピュータは、ネットワーク接続コンピュータリスト１００の最後のＭＡＣアドレスであるため、ステップＡ７の処理後、終了する。

以上の処理によって、図５に示すソフトウェア資産管理漏れリスト３００が作成される。

【００５９】

以上説明したように、本実施形態のネットワークを利用したソフトウェア資産管理漏れ検出システムによれば、ソフトウェア資産管理から漏れているコンピュータを容易に洗い出すことが可能となる。

また、従来のソフトウェア資産管理システムを大幅に変更することなくソフトウェア資産管理情報の漏れを防止することが可能となる。

その結果、ＯＳやソフトウェアのバージョンやパッチ適用状態等が不明なコンピュータを検出し、パッチ適用状態が最新ではなくセキュリティホールとなりうるコンピュータがネットワークに接続されたままになることを防止することが可能となる。

さらに、ネットワーク接続コンピュータリストとソフトウェア資産管理リストを適切な間隔で定期的に更新して比較することにより、ソフトウェア資産管理外のコンピュータや不正なコンピュータが接続された場合に、これを早期に発見することが可能となる。

【００６０】

［第二実施形態］

次に、本発明の第二実施形態について、図３、及び図６～図８を参照して説明する。図６は、本実施形態のネットワークを利用したソフトウェア資産管理漏れ検出システムにおける処理手順を示すフローチャートである。図７は、同システムにおけるネットワーク接続コンピュータリスト及びソフトウェア資産管理リストの具体例を示す図である。図８は、同システムにおけるソフトウェア資産管理漏れ検出リストと、非使用状態となっているコンピュータのリスト、すなわち非使用コンピュータリストの具体例を示す図である。

本実施形態は、以前使用されていたが、現在は使用されていないコンピュータを洗い出すことができる点で第一実施形態と異なる。

【００６１】

図６のフローチャートにおける動作手順は、図３のフローチャートにおけるネットワーク接続コンピュータリスト１００とソフトウェア資産管理リスト２００との関係を逆転させたものである。

これによって、ソフトウェア資産管理リストに含まれているが、ネットワーク接続コンピュータリストには含まれていないコンピュータを検出することが可能となり、これを既に利用されていないコンピュータと判断することができる。

また、ソフトウェア資産管理漏れ検出サーバ３０に、図３のフローチャートの

処理終了後に図６のフローチャートの処理を行わせることによって、ソフトウェア資産管理漏れコンピュータリスト３００、及び非使用コンピュータリスト４００を共に生成することができる。

すなわち、ソフトウェア資産管理から漏れているコンピュータを検出するとともに、現在未使用のソフトウェアの一覧を取得することが可能となり、ソフトウェア資産管理をより厳密に行うことが容易となる。

【００６２】

次に、図７に示すネットワーク接続リスト１００、及びソフトウェア資産管理リスト２００を用いて、図３のフローチャートと図６のフローチャートを連続して処理する場合の動作について、具体的に説明する。

図７のリストは、図４のリストのうち、ソフトウェア資産管理リスト２００に、ネットワーク接続コンピュータリスト１００に含まれていない２台分のコンピュータの情報を追加したものであり、ネットワーク接続コンピュータリスト１００は図４のものと同一である。

つまり、図７のリストにおいて、ネットワーク接続コンピュータリスト１００に含まれており、ソフトウェア資産管理リスト２００に含まれていないコンピュータは図４のリストと同様となる。

したがって、図７のリストを用いた場合に、ソフトウェア資産管理漏れリスト３００に追加されるコンピュータは、図４のリストを用いた場合と同じになるため、図３のフローチャートによるソフトウェア資産管理漏れリスト３００を生成する処理の詳細な動作の説明は省略する。

【００６３】

続いて、図３のフローチャートの処理後に実行される、図６のフローチャートの処理について詳細に説明する。

まず、ソフトウェア資産管理リスト２００からリストの先頭のＭＡＣアドレス「００：００：４ｃ：５５：５５：５５」を取り出し（ステップＢ１）、ネットワーク接続コンピュータリスト１００からリストの先頭のＭＡＣアドレス「００：００：４ｃ：１１：１１：１１」を取り出す（ステップＢ２）。

次に、取り出したＭＡＣアドレスの比較を行う（ステップＢ３）。この場合、

それぞれのリストから取り出したＭＡＣアドレスが異なっているため、ステップＢ４に進む。

【００６４】

そして、ネットワーク接続コンピュータリスト１００から取り出したＭＡＣアドレスがリスト１００の最後のものかを判断する（ステップＢ４）。この場合はリストの最後ではないので、リストの次のＭＡＣアドレス「００：００：４ｃ：２２：２２：２２」を取り出して（ステップＢ５）、ステップＢ３に戻る。

次のステップＢ３でのＭＡＣアドレスの比較も同様にＭＡＣアドレスが異なっているため、ステップＢ４、ステップＢ５の順番に処理が進み、ネットワーク接続コンピュータリスト１００の次のＭＡＣアドレス「００：００：４ｃ：５５：５５：５５」を取り出してステップＢ３に戻る。

【００６５】

次のステップＢ３でのＭＡＣアドレスの比較では、ＭＡＣアドレスが一致しているため、ステップＢ７に進む。

そして、ソフトウェア資産管理リスト２００から取り出したＭＡＣアドレスがリスト２００の最後のものかを判断する（ステップＢ７）。この場合はリスト２００の最後のものではないため、ステップＢ８に進む。

そして、リストの次のＭＡＣアドレス「００：００：４ｃ：３３：３３：３３」を取り出して（ステップＢ８）、ステップＢ２に戻る。

【００６６】

これ以降の動作は、ソフトウェア資産管理リスト２００から取り出したＭＡＣアドレスが「００：００：４ｃ：５５：５５：５５」の場合と同様であるが、ネットワーク接続コンピュータリスト１００にはＭＡＣアドレス「００：００：４ｃ：３３：３３：３３」のコンピュータが登録されていない。

このため、ネットワーク接続コンピュータリスト１００から取り出したＭＡＣアドレスが「００：００：４ｃ：ｂｂ：ｂｂ：ｂｂ」の時、ステップＢ４において、これはネットワーク接続コンピュータリスト１００の最後のＭＡＣアドレスのため、ステップＢ６に進み、非使用コンピュータリスト４００に、ＭＡＣアドレスが「００：００：４ｃ：３３：３３：３３」のコンピュータの情報が追加さ

れる（ステップＢ６）。

【００６７】

ソフトウェア資産管理リスト２００に登録されているコンピュータのうち、ＭＡＣアドレスが「００：００：４ｃ：１１：１１：１１」、「００：００：４ｃ：７７：７７：７７」のコンピュータに関しては、ネットワーク接続コンピュータリスト１００にも登録されているため、ＭＡＣアドレスが、「００：００：４ｃ：５５：５５：５５」のコンピュータの時と同様の動作となる。

また、ＭＡＣアドレスが「００：００：４ｃ：８８：８８：８８」のコンピュータに関しては、ネットワーク接続コンピュータリスト１００に登録されていないため、ＭＡＣアドレスが「００：００：４ｃ：３３：３３：３３」のコンピュータの時と同様の動作となる。

【００６８】

そして、リスト２００におけるＭＡＣアドレスが「００：００：４ｃ：７７：７７：７７」のコンピュータについては、ソフトウェア資産管理リスト２００の最後のＭＡＣアドレスであるため、ステップＢ７の処理後、終了する。

図８は、このようにして生成されたソフトウェア資産管理漏れリスト３００、及び非使用コンピュータリスト４００を示している。

【００６９】

以上説明したように、本実施形態のネットワークを利用したソフトウェア資産管理漏れ検出システムによれば、ソフトウェア資産管理漏れリストのみならず、非使用コンピュータリストを生成することができ、すでに使用されていないコンピュータを洗い出すことが可能となる。

すなわち、ソフトウェア資産管理から漏れているコンピュータを検出するとともに、現在未使用のソフトウェアの一覧を取得することが可能となり、ソフトウェア資産管理をより厳密に行うことが容易となる。

【００７０】

［第三実施形態］

次に、本発明の第三実施形態について、図９を参照して説明する。同図は、本実施形態のネットワークを利用したソフトウェア資産管理漏れ検出サーバの構成

を示すブロック図である。

本実施形態は、ソフトウェア資産管理漏れ検出リスト３００や非使用コンピュータリスト４００の作成を、一台のサーバにより行うことができる点で第一，及び第二実施形態と異なる。

【００７１】

すなわち、図９において、資産統合管理サーバ１０００は、図１におけるネットワーク接続管理サーバ１０、ソフトウェア資産管理サーバ２０、ソフトウェア資産管理漏れ検出サーバ３０の３つのサーバに分かれている構成を、一つのサーバにまとめたものである。

図９において、ネットワーク接続管理部１０１０が図１のネットワーク接続管理サーバ１０の機能を、ソフトウェア資産管理部１０２０がソフトウェア資産管理サーバ２０の機能を、そしてソフトウェア資産管理漏れ検出部１０３０がソフトウェア資産管理漏れ検出サーバ３０の機能を実現している。

このように、本発明を実施する際には、各機能毎にサーバを設置してもよく、また各機能を１台のサーバで実現してもよい。

【００７２】

［第四実施形態］

次に、本発明の四実施形態について、図１０を参照して説明する。同図は、本実施形態のネットワークを利用したソフトウェア資産管理漏れ検出サーバの構成を示すブロック図である。

本実施形態は、ソフトウェア資産管理漏れリスト３００又は未使用コンピュータリスト４００の作成にあたり、ネットワーク接続コンピュータリスト１００及びソフトウェア資産管理リスト２００をそれぞれソートした後に用いる点で第三実施形態と異なる。

【００７３】

すなわち、図１０において、資産統合管理サーバ１０００は、第三実施形態における構成に加えてリスト前処理部１０４０を有している。

このリスト前処理部１０４０において、ネットワーク接続コンピュータリスト１００とソフトウェア資産管理情報リスト２００をそれぞれＭＡＣアドレスに対

して昇順、又は降順にソートすることにより、ソフトウェア資産管理漏れ検出部１０３０では逐次探索アルゴリズムを利用する処理の代わりに、例えば二分探索アルゴリズムを利用した処理を行うことが可能となる。

その結果、ソフトウェア資産管理漏れリスト３００と未使用コンピュータリスト４００を生成する処理を高速化することが可能となる。

【００７４】

このように、本発明を実施する際には、図１におけるネットワークアドレスをキーとしたリスト比較処理が可能なアルゴリズムであれば、どのようなアルゴリズムを用いてもよい。

また、このようなリスト前処理を、第一実施形態又は第二実施形態において、行うようにすることももちろん可能である。

このとき、リスト前処理を、ネットワーク接続管理サーバ１０において、ネットワーク接続コンピュータリスト１００に対して行うとともに、ソフトウェア資産管理サーバ２０において、ソフトウェア資産管理リスト２００に対して行うようにすることができる。

また、リスト前処理をソフトウェア資産管理漏れ検出サーバ３０において、ネットワーク接続コンピュータリスト１００及びソフトウェア資産管理リスト２００の双方に対して行うようにしてもよい。

【００７５】

上記の実施形態におけるソフトウェア資産管理漏れの検出や、ソフトウェア資産管理漏れ検出リストの作成等は、ネットワークを利用したソフトウェア資産管理漏れ検出プログラムにより実行される。

このネットワークを利用したソフトウェア資産管理漏れ検出プログラムは、コンピュータの各構成要素に指令を送り、所定の処理、例えば、ソフトウェア資産管理漏れの検出処理や、ソフトウェア資産管理漏れ検出リストの作成処理等を行わせる。

これによって、これらの処理は、ネットワークを利用したソフトウェア資産管理漏れ検出プログラムとコンピュータとが協働したネットワークを利用したソフトウェア資産管理漏れ検出サーバ３０などにより実現される。

【００７６】

なお、ネットワークを利用したソフトウェア資産管理漏れ検出プログラムは、コンピュータのＲＯＭやハードディスクに記憶させる他、コンピュータ読み取り可能な記録媒体、たとえば、外部記憶装置及び可搬記録媒体等に格納することができる。

外部記憶装置とは、磁気ディスク等の記録媒体を内蔵し、例えばネットワークを利用したソフトウェア資産管理漏れ検出サーバ３０などに外部接続される記憶増設装置をいう。一方、可搬記録媒体とは、記録媒体駆動装置（ドライブ装置）に装着でき、かつ、持ち運び可能な記録媒体であって、たとえば、ＣＤ－ＲＯＭ、フレキシブルディスク、メモリカード、光磁気ディスク等をいう。

【００７７】

そして、記録媒体に記録されたプログラムは、コンピュータのＲＡＭにロードされて、ＣＰＵにより実行される。この実行により、上述した本実施形態のネットワークを利用したソフトウェア資産管理漏れ検出サーバ３０の手段が実現される。

さらに、コンピュータでネットワークを利用したソフトウェア資産管理漏れ検出プログラムをロードする場合、他のコンピュータで保有されたネットワークを利用したソフトウェア資産管理漏れ検出プログラムを、通信回線を利用して自己の有するＲＡＭや外部記憶装置にダウンロードすることもできる。

このダウンロードされたネットワークを利用したソフトウェア資産管理漏れ検出プログラムも、ＣＰＵにより実行され、本実施形態のソフトウェア資産管理漏れの検出処理や、ソフトウェア資産管理漏れ検出リストの作成処理等を実現する。

【００７８】

なお、本発明は以上の実施形態に限定されるものではなく、本発明の範囲内において、種々の変更実施が可能であることは言うまでもない。

例えば、ネットワーク接続コンピュータリスト１００及びソフトウェア資産管理リスト２００を比較する際のキーとして、ＭＡＣアドレス以外のネットワークアドレスやコンピュータを一意に識別可能な他のキーを利用するなど適宜設計変

更することのできるものである。

【００７９】

【発明の効果】

以上のように、本発明によれば、ソフトウェア資産管理情報とは別にネットワークに接続されているコンピュータを漏れなく含むリストを作成し、ネットワークアドレスなどネットワーク上でコンピュータを一意に識別することが可能な情報を用いることで、ソフトウェア資産管理から漏れているコンピュータを見つけ出すことができる。

このため、ソフトウェア資産管理から漏れているコンピュータを容易に洗い出すことが可能となる。

【００８０】

また、ネットワークに接続されているコンピュータを漏れなく含むリストを作成する手段を、従来のソフトウェア資産管理システムから独立して構成し、ソフトウェア資産管理漏れのコンピュータを検出することができる。

そして、このソフトウェア資産管理漏れのコンピュータに対して、従来のソフトウェア資産管理システムを適用することが可能となる。

このため、従来のソフトウェア資産管理システムを大幅に変更することなくソフトウェア資産管理情報の漏れを防止することが可能となる。

【００８１】

その結果、ＯＳやソフトウェアのバージョンやパッチ適用状態等も同時に管理するソフトウェア資産管理において、ネットワークに接続されたコンピュータを漏れなく含んだリストを用いることによって、管理漏れを防ぐことが可能となる。

このため、ＯＳやソフトウェアのバージョンやパッチ適用状態等が不明なコンピュータを検出し、パッチ適用状態が最新ではなくセキュリティホールとなりうるコンピュータがネットワークに接続されたままになることを防止することが可能となる。

【００８２】

また、ネットワーク接続コンピュータリストとソフトウェア資産管理リストを

１日ごとなど適切な間隔で定期的に更新して比較することにより、新規にネットワークに接続されたコンピュータがソフトウェア資産管理下にあるかどうかを確認することができる。

このため、ソフトウェア資産管理外のコンピュータや不正なコンピュータが接続された場合、管理外コンピュータとして早期に発見することが可能となる。

【００８３】

さらに、ソフトウェア資産管理漏れリストのみならず、非使用コンピュータリストを生成することができ、すでに使用されていないコンピュータを洗い出すことが可能となる。

すなわち、ソフトウェア資産管理から漏れているコンピュータを検出するとともに、現在未使用のソフトウェアの一覧を取得することが可能となり、ソフトウェア資産管理をより厳密に行うことが容易となる。

【００８４】

加えて、ネットワークを利用したソフトウェア資産管理漏れ検出プログラムは、ネットワークを利用したソフトウェア資産管理漏れ検出サーバの制御部へ所定の指令を送ることにより、このソフトウェア資産管理漏れの検出機能や、ソフトウェア資産管理漏れ検出リストの作成機能等を実現させることができる。

これによって、これらの機能等は、ネットワークを利用したソフトウェア資産管理漏れ検出プログラムとネットワークを利用したソフトウェア資産管理漏れ検出サーバとが協働して実現することが可能である。

【図面の簡単な説明】

【図１】

本発明の第一実施形態のネットワークを利用したソフトウェア資産管理漏れ検出システムの構成を示すブロック図である。

【図２】

本発明の第一実施形態のネットワークを利用したソフトウェア資産管理漏れ検出システムにおけるネットワーク接続コンピュータリスト及びソフトウェア資産管理リストを示す図である。

【図３】

本発明の第一実施形態のネットワークを利用したソフトウェア資産管理漏れ検出システムにおける処理手順を示すフローチャートである。

【図４】

本発明の第一実施形態のネットワークを利用したソフトウェア資産管理漏れ検出システムにおけるネットワーク接続コンピュータリスト及びソフトウェア資産管理リストの具体例を示す図である。

【図５】

本発明の第一実施形態のネットワークを利用したソフトウェア資産管理漏れ検出システムにおけるソフトウェア資産管理漏れリストの具体例を示す図である。

【図６】

本発明の第二実施形態のネットワークを利用したソフトウェア資産管理漏れ検出システムにおける処理手順を示すフローチャートである。

【図７】

本発明の第二実施形態のネットワークを利用したソフトウェア資産管理漏れ検出システムにおけるネットワーク接続コンピュータリスト及びソフトウェア資産管理リストの具体例を示す図である。

【図８】

本発明の第二実施形態のネットワークを利用したソフトウェア資産管理漏れ検出システムにおけるソフトウェア資産管理漏れリスト及び非使用コンピュータリストの具体例を示す図である。

【図９】

本発明の第三実施形態のネットワークを利用したソフトウェア資産管理漏れ検出サーバの構成を示すブロック図である。

【図１０】

本発明の第四実施形態のネットワークを利用したソフトウェア資産管理漏れ検出サーバの構成を示すブロック図である。

【符号の説明】

１０　ネットワーク接続管理サーバ

１００　ネットワーク接続コンピュータリスト

２０　ソフトウェア資産管理サーバ

２００　ソフトウェア資産管理リスト

３０　ソフトウェア資産管理漏れ検出サーバ

３００　ソフトウェア資産管理漏れリスト

４００　非使用コンピュータリスト

１０００　資産統合管理サーバ

１０１０　ネットワーク接続管理部

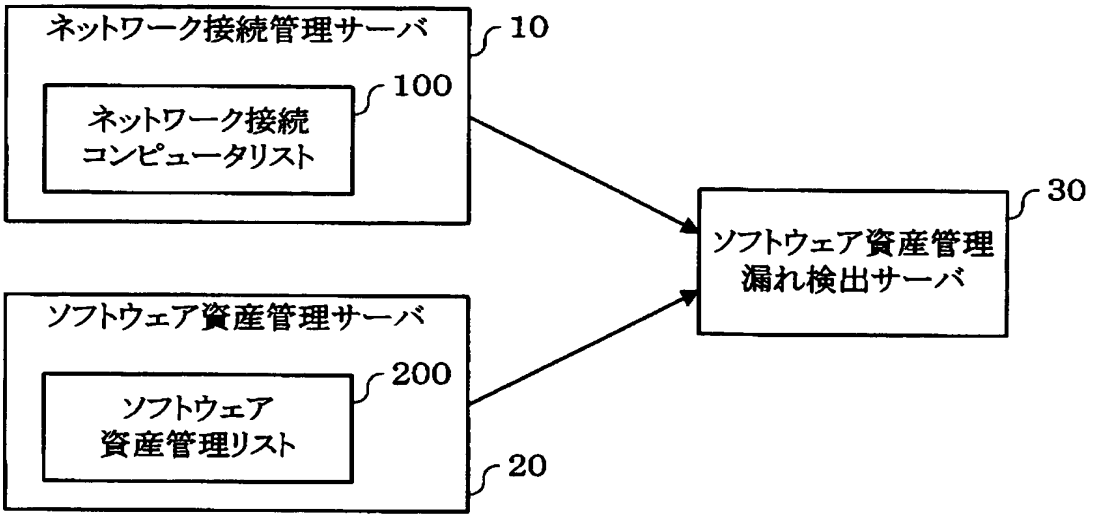
１０２０　ソフトウェア資産管理部

１０３０　ソフトウェア資産管理漏れ検出部

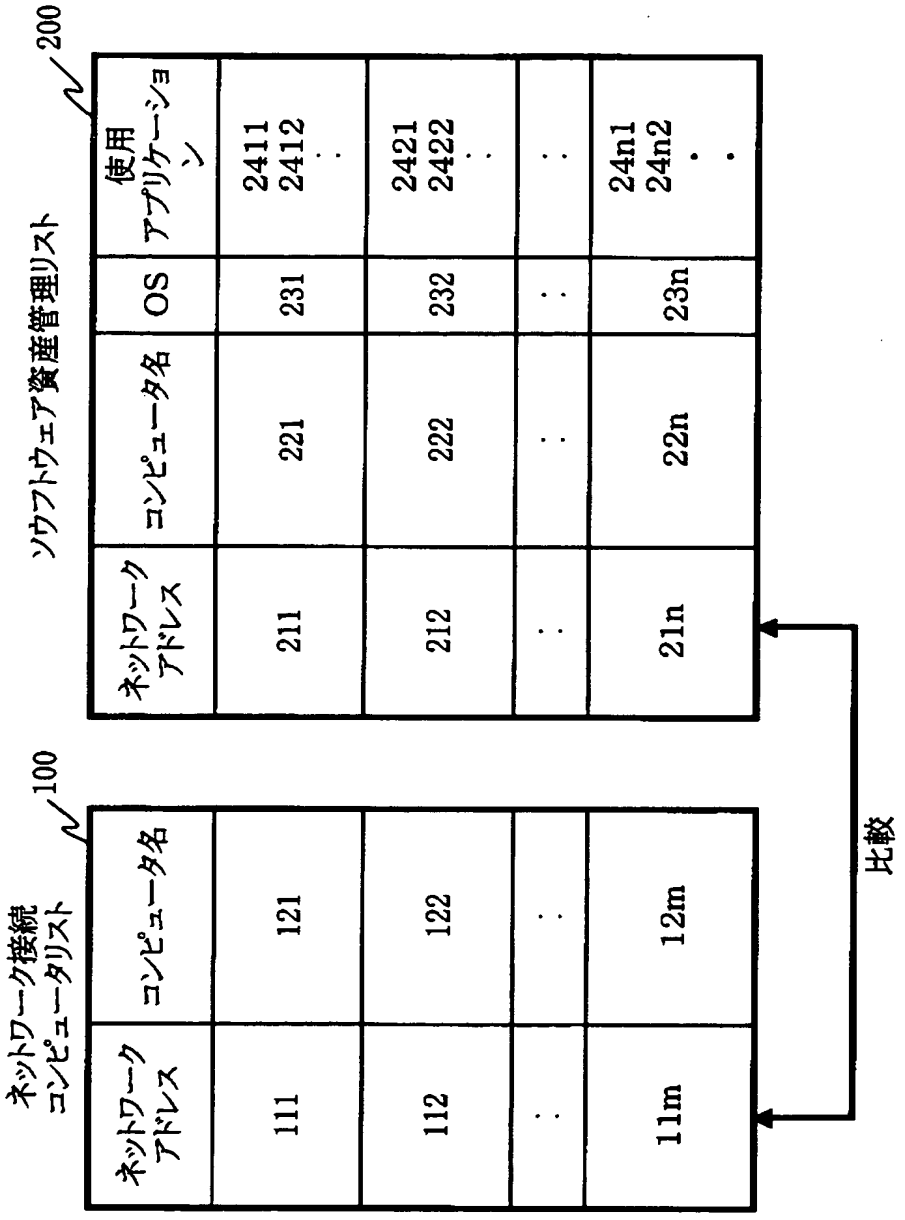
１０４０　リスト前処理部

【書類名】　図面

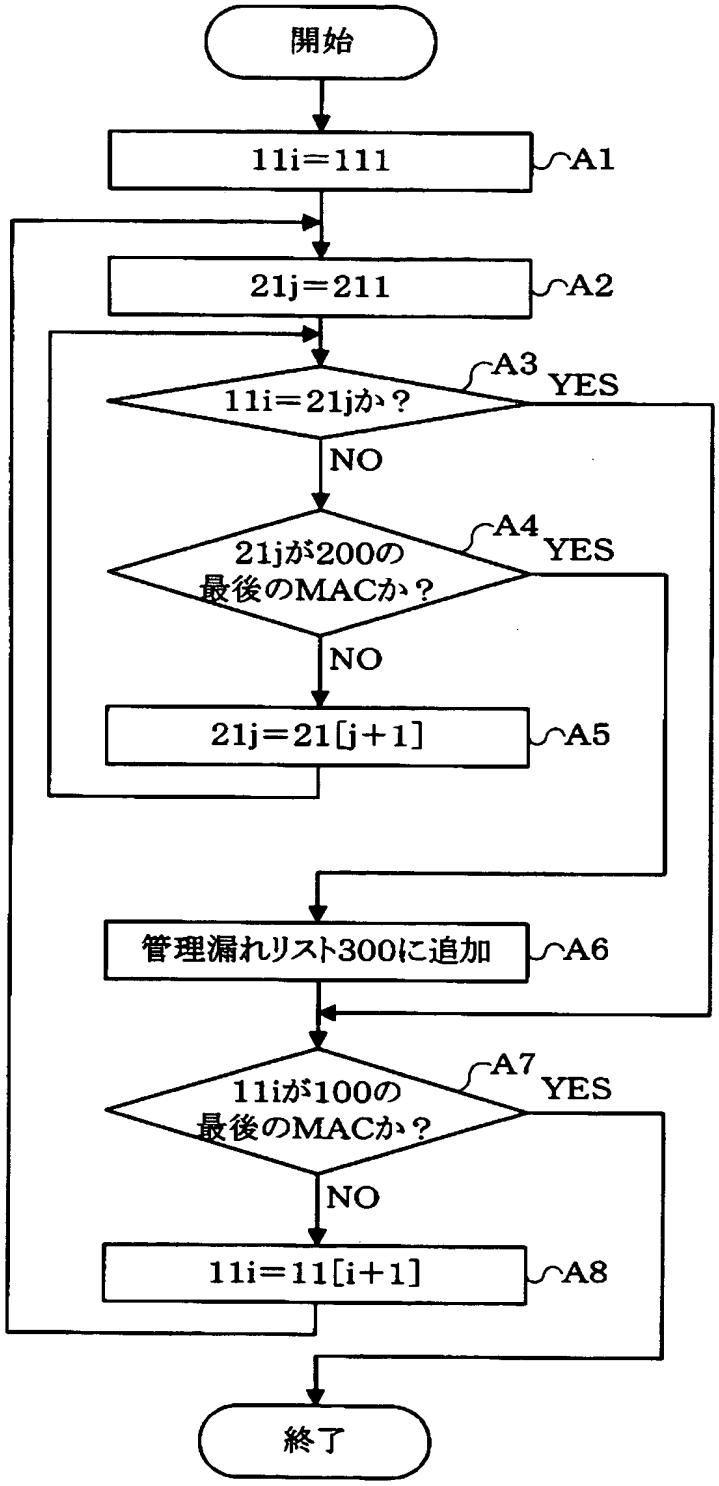
【図１】


ネットワーク接続管理サーバ
10
ネットワーク接続
コンピュータリスト
100
ソフトウェア資産管理
漏れ検出サーバ
30
ソフトウェア資産管理サーバ
ソフトウェア
資産管理リスト
200
20

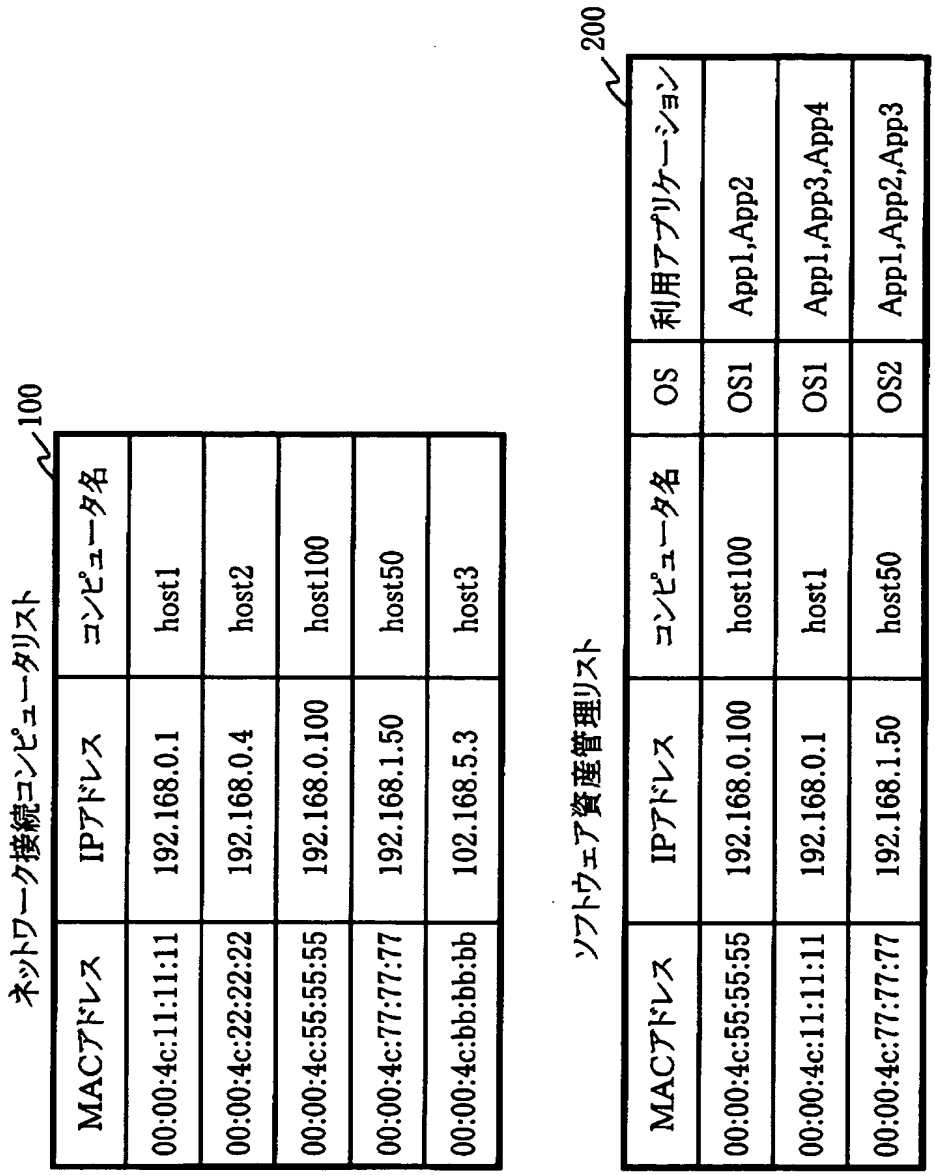
【図２】


ネットワーク接続コンピュータリスト
100
ネットワークアドレス
コンピュータ名
111
121
112
122
11m
12m
比較
ソウフトウェア資産管理リスト
200
ネットワークアドレス
コンピュータ名
OS
使用アプリケーション
211
221
231
2411
2412
212
222
232
2421
2422
21n
22n
23n
24n1
24n2

【図３】


開始
11i=111
A1
21j=211
A2
A3
11i=21jか？
YES
NO
A4
21jが200の
最後のMACか？
YES
NO
21j=21[j+1]
A5
管理漏れリスト300に追加
A6
A7
11iが100の
最後のMACか？
YES
NO
11i=11[i+1]
A8
終了

【図４】



ネットワーク接続コンピュータリスト　100

MACアドレス	IPアドレス	コンピュータ名
00:00:4c:11:11:11	192.168.0.1	host1
00:00:4c:22:22:22	192.168.0.4	host2
00:00:4c:55:55:55	192.168.0.100	host100
00:00:4c:77:77:77	192.168.1.50	host50
00:00:4c:bb:bb:bb	102.168.5.3	host3

ソフトウェア資産管理リスト　200

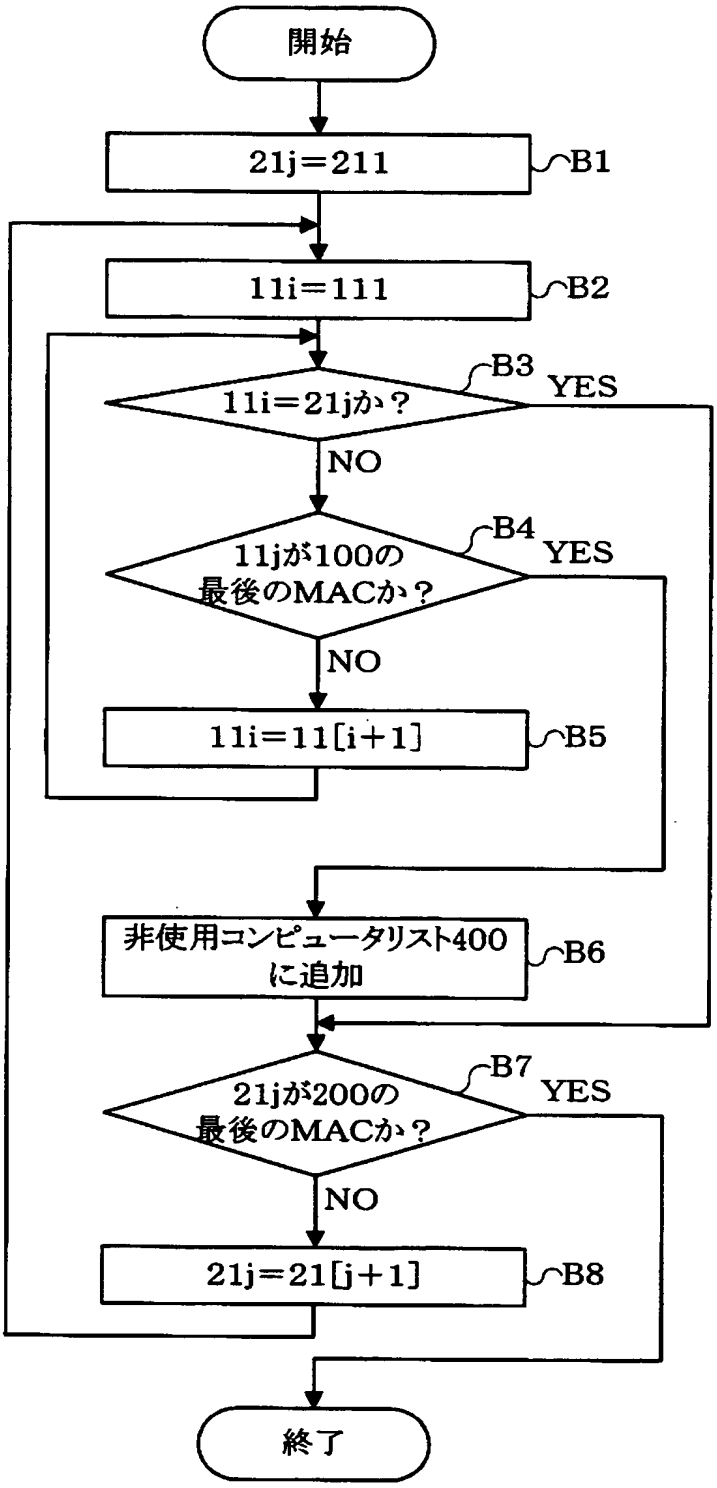
MACアドレス	IPアドレス	コンピュータ名	OS	利用アプリケーション
00:00:4c:55:55:55	192.168.0.100	host100	OS1	App1,App2
00:00:4c:11:11:11	192.168.0.1	host1	OS1	App1,App3,App4
00:00:4c:77:77:77	192.168.1.50	host50	OS2	App1,App2,App3

【図５】

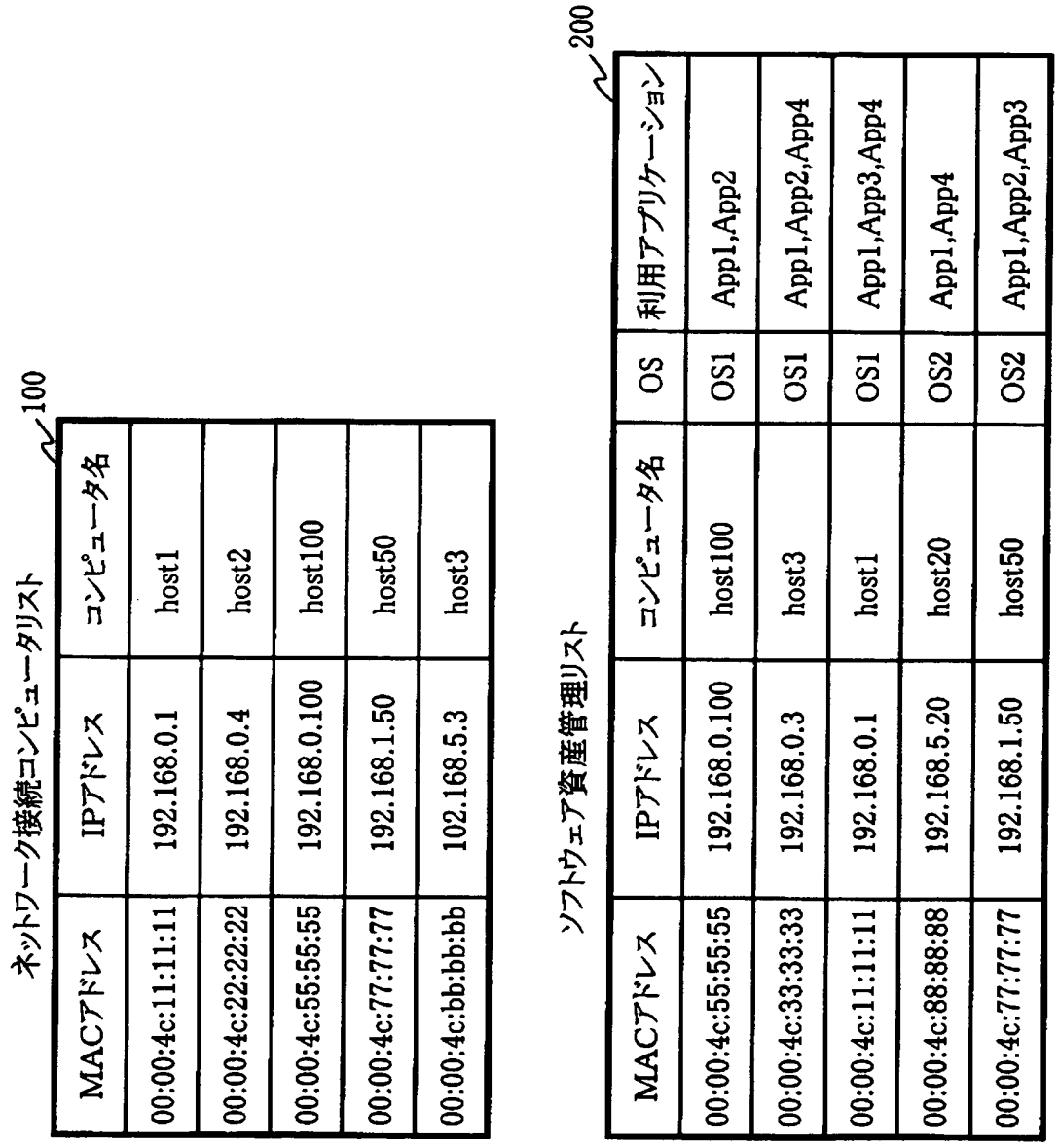
ソフトウェア資産管理漏れリスト　300

MACアドレス	IPアドレス	コンピュータ名
00:00:4c:22:22:22	192.168.0.4	host2
00:00:4c:bb:bb:bb	102.168.5.3	host3

【図６】


開始
21j=211
B1
11i=111
B2
B3
11i=21jか？
YES
NO
B4
11jが100の
最後のMACか？
YES
NO
11i=11[i+1]
B5
非使用コンピュータリスト400
に追加
B6
B7
21jが200の
最後のMACか？
YES
NO
21j=21[j+1]
B8
終了

【図７】



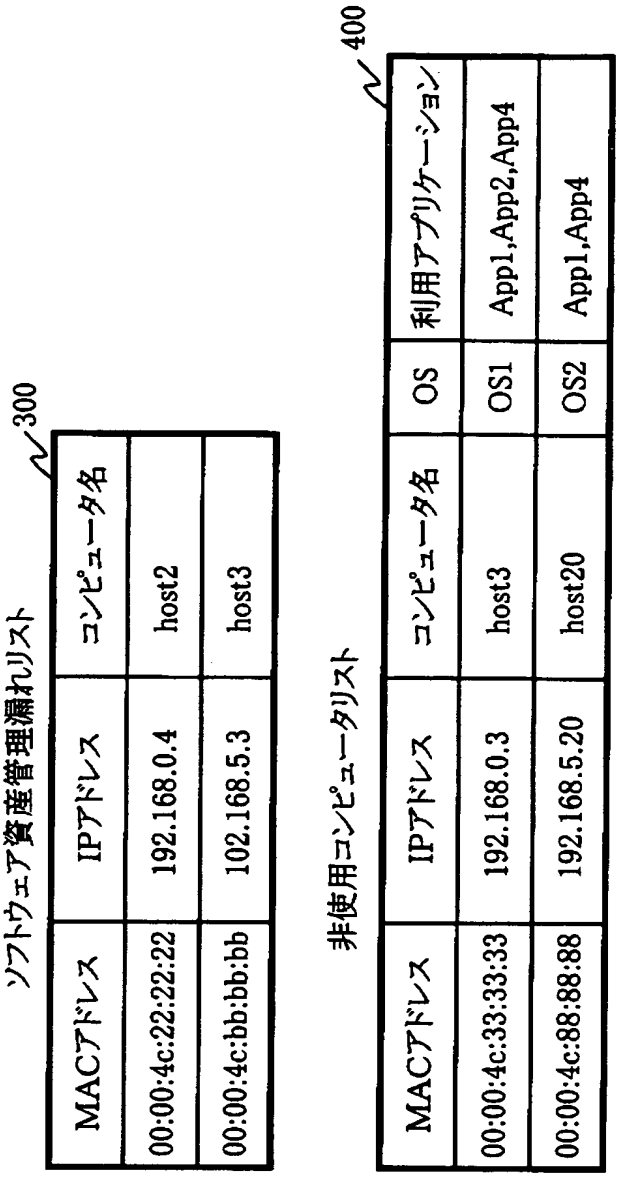
ネットワーク接続コンピュータリスト　100

MACアドレス	IPアドレス	コンピュータ名
00:00:4c:11:11:11	192.168.0.1	host1
00:00:4c:22:22:22	192.168.0.4	host2
00:00:4c:55:55:55	192.168.0.100	host100
00:00:4c:77:77:77	192.168.1.50	host50
00:00:4c:bb:bb:bb	102.168.5.3	host3

ソフトウェア資産管理リスト　200

MACアドレス	IPアドレス	コンピュータ名	OS	利用アプリケーション
00:00:4c:55:55:55	192.168.0.100	host100	OS1	App1,App2
00:00:4c:33:33:33	192.168.0.3	host3	OS1	App1,App2,App4
00:00:4c:11:11:11	192.168.0.1	host1	OS1	App1,App3,App4
00:00:4c:88:88:88	192.168.5.20	host20	OS2	App1,App4
00:00:4c:77:77:77	192.168.1.50	host50	OS2	App1,App2,App3

【図８】



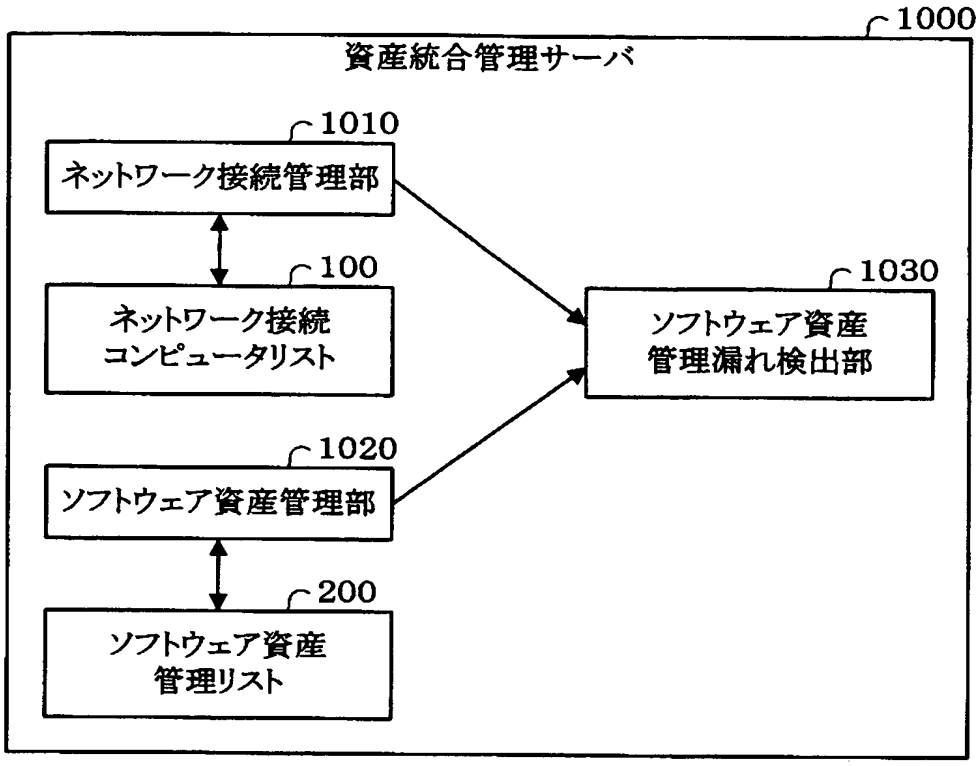
ソフトウェア資産管理漏れリスト　300

MACアドレス	IPアドレス	コンピュータ名
00:00:4c:22:22:22	192.168.0.4	host2
00:00:4c:bb:bb:bb	102.168.5.3	host3

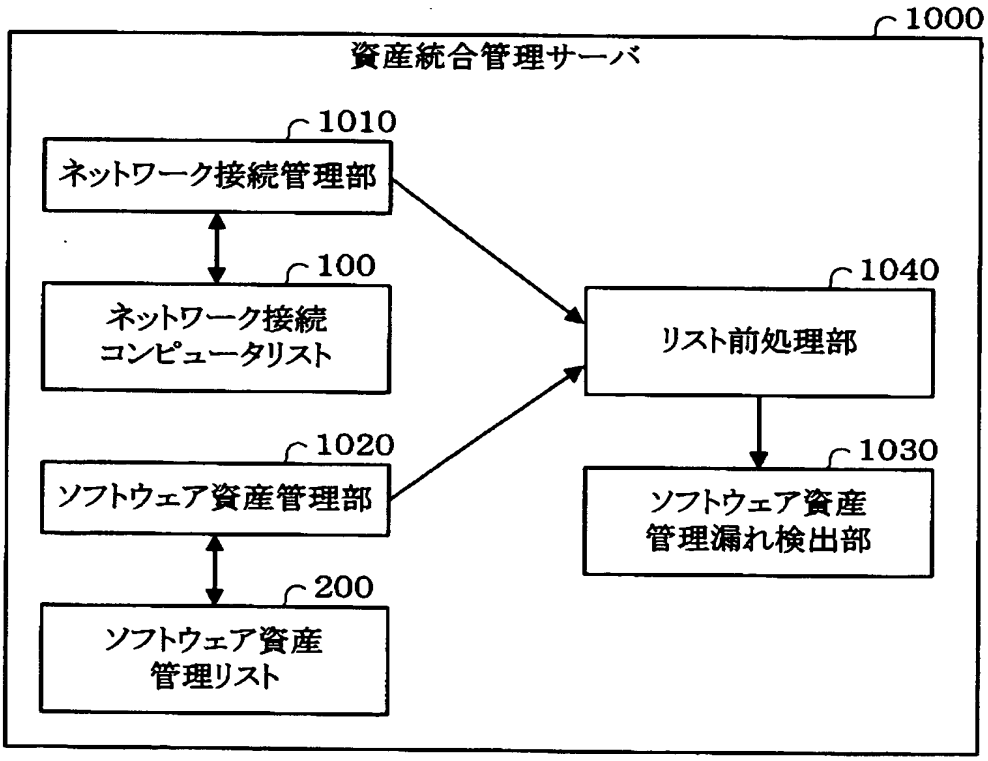
非使用コンピュータリスト　400

MACアドレス	IPアドレス	コンピュータ名	OS	利用アプリケーション
00:00:4c:33:33:33	192.168.0.3	host3	OS1	App1,App2,App4
00:00:4c:88:88:88	192.168.5.20	host20	OS2	App1,App4

【図９】


1000
資産統合管理サーバ
1010
ネットワーク接続管理部
100
ネットワーク接続
コンピュータリスト
1030
ソフトウェア資産
管理漏れ検出部
1020
ソフトウェア資産管理部
200
ソフトウェア資産
管理リスト

【図１０】


1000
資産統合管理サーバ
1010
ネットワーク接続管理部
100
ネットワーク接続
コンピュータリスト
1040
リスト前処理部
1030
ソフトウェア資産
管理漏れ検出部
1020
ソフトウェア資産管理部
200
ソフトウェア資産
管理リスト

【書類名】　要約書

【要約】

【課題】　コンピュータごとに、その基本情報及びインストールされているソフトウェア、修正パッチの適用状況を管理するソフトウェア資産管理から、管理すべきコンピュータが漏れることを防止する。

【解決手段】　所定のネットワークに接続された全てのコンピュータについて、各コンピュータを特定するための情報を保有するネットワーク接続コンピュータリスト１００と、ソフトウェア資産管理の管理対象となっている全てのコンピュータについて、各コンピュータを特定するための情報を保有するソフトウェア資産管理リスト２００とにもとづいて、ネットワーク接続コンピュータリスト１００に存在し、かつ、ソフトウェア資産管理リスト２００に存在しないコンピュータを抽出し、ソフトウェア資産管理漏れのコンピュータのリスト３００を作成することを特徴とするネットワークを利用したソフトウェア資産管理漏れ検出方法。

【選択図】　図１

出　願　人　履　歴　情　報

識別番号　　［０００００４２３７］

１．変更年月日　　１９９０年　８月２９日
［変更理由］　　新規登録
住　所　　東京都港区芝五丁目７番１号
氏　名　　日本電気株式会社

特願２００２－３４２７３５

出　願　人　履　歴　情　報

識別番号　　［３９０００１３９５］

１．変更年月日　　２００１年１１月２８日
［変更理由］　　名称変更
住　所　　大阪府大阪市中央区城見１丁目４番２４号
氏　名　　エヌイーシーシステムテクノロジー株式会社